3 The fundamentals: Algorithms, the integers, and matrices

3.4 The integers and division

This section introduces the basics of number theory (number theory is the part of mathematics involving integers and their properties).

1. $a|b$ if $b = a\,k$, for some integer k (note that $a|b$ is not the fraction b/a, but it rather shows that a is a factor of b)

2. $a \not| b$ if a is not a factor of b. Examples: $3|18$ but $3 \not| 20$.

3. <u>properties of $a|b$</u>: (you should be able to prove them) Let $a, b, c \in \mathbb{Z}$. Then:

   - $(a|b \;\wedge\; a|c) \;\;\rightarrow\;\; a|(b+c)$

   - $a|b \;\;\rightarrow\;\; a|(bc), \;\; \forall c \in \mathbb{Z}$

   - $(a|b \;\wedge\; b|c) \;\;\rightarrow\;\; a|c$

   - $(a|b \;\wedge\; a|c) \;\;\rightarrow\;\; a|(mb+nc), \;\; \forall m, n \in \mathbb{Z}$

4. <u>Division algorithm</u>: $\forall a, d \in \mathbb{Z}$, with $d > 0 \Rightarrow \exists! \;\; q, r \;\; (0 \leq r < d)$ such that $a = dq + r$

5. in the equation above, a is called the <u>dividend</u>, d is the <u>divisor</u>, q is the <u>quotient</u>, and r is the <u>remainder</u>. Note that a and d are the given integers, and q and r are the unique two integers that make the division algorithm work for the given a and d. Example: Given 14 and 5, find the quotient and the remainder: $14 = 5 \cdot 2 + 4$, so $q = 2$ and $r = 4$ and they are unique for the pair of numbers 14 and 5. We then have that $2 = 14 \text{ div } 5$ and $4 = 14 \bmod 5$

6. $a \,\underline{\bmod}\, m$ gives the reminder when a is divided by m

7. modular arithmetics: $a \equiv b (\bmod m) \iff m|(a-b)$. This means that both a and b have the same reminder when they are divided by m.

8. modular arithmetics: $a \not\equiv b(\bmod m) \iff m \nmid (a-b)$
Example: $14 \equiv 4(\bmod 5)$ since $5|(14-4)$,
however $14 \not\equiv 2(\bmod 5)$ since $5 \nmid (14-2)$

9. **Theorem:** $a \equiv b(\bmod m)$ **iff** $a \,\underline{\text{mod}}\, m = b \,\underline{\text{mod}}\, m$ (note that when $(\bmod m)$ is in the equation, then we use the symbol $\equiv$, but if we use the $\underline{\text{mod}}\, m$, then we use the symbol $=$ since we're talking about remainders.)

10. modular arithmetic operations:

    - addition: $\Big(a \,\underline{\text{mod}}\, m + b \,\underline{\text{mod}}\, m\Big) \,\underline{\text{mod}}\, m = (a+b) \,\underline{\text{mod}}\, m$

    - subtraction: $\Big(a \,\underline{\text{mod}}\, m - b \,\underline{\text{mod}}\, m\Big) \,\underline{\text{mod}}\, m = (a-b) \,\underline{\text{mod}}\, m$

    - multiplication: $\Big(a \,\underline{\text{mod}}\, m \cdot b \,\underline{\text{mod}}\, m\Big) \,\underline{\text{mod}}\, m = (a \cdot b) \,\underline{\text{mod}}\, m$

11. not true for division (division is not defined for modular arithmetic. We define cancellation, and one can only cancel if the number that one cancels by is relatively prime to m–see Section 3.7)

12. if $a \equiv b(\bmod m)$ and $c \equiv d(\bmod m)$, then
    - $a + c \equiv b + d \,(\bmod m)$
    - $a - c \equiv b - d \,(\bmod m)$
    - $a \cdot c \equiv b \cdot d \,(\bmod m)$
    - $a\alpha \equiv b\alpha \,(\bmod m)$, for $\alpha > 0, m \geq 2, \alpha \in \mathbb{Z}$
    - $a\alpha \equiv b\alpha \,(\bmod m\alpha)$, for $\alpha > 0, m \geq 2, \alpha \in \mathbb{Z}$

13. Applications: hashing functions, pseudo random numbers, code generating in cryptography

3.5 Primes and greatest common divisors

1. a prime p is an integer greater than 1 whose only positive factors are 1 and p (note that 2 is the smallest prime number, and the only even prime number). If an integer greater than 1 is not prime, then it is a composite number. Note that only integers that are greater than or equal to 2 are either primes or composite.

2. if n is a composite integer, then n has prime divisors less than or equal to $\sqrt{n}$ (so in searching for divisors in a factorization of n, one should only look up to $\sqrt{n}$)

3. Fundamental Theorem of Arithmetic: every positive integer greater than 1 can be uniquely written as product of primes (where the factors are arranged in an increasing order)
i.e.: $n = p_1 \cdot p_2 \cdot \ldots \cdot p_\alpha$, where $p_i \leq p_{i+1}$ for $1 \leq i \leq \alpha - 1$

4. there are infinitely many primes (look at the construction in the proof)

5. The prime number theorem: The ratio of the number of primes not exceeding x and $\frac{x}{\ln x}$ approaches 1 as $x \to \infty$. Proof is complicated, but its usefulness comes in estimating the odds of choosing a random number that is prime.

6. gcd of two numbers = greatest common divisor: $\gcd(12, 30) = 6$

7. lcm of two numbers = least common multiple: $\text{lcm}(12, 30) = 60$

8. a and b are relatively prime (or also called coprimes) if $\gcd(a, b) = 1$:
The numbers 7 and 9 are relatively prime

9. the integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if all pairs of them are relatively prime (i.e. $\gcd(a_i, a_j) = 1, \forall i, j$ with $1 \leq i \neq j \leq n$).

10. $ab = \gcd\ (a, b) \cdot\ \text{lcm}(a, b)$

3.6 Integers and algorithms

This section presents techniques for transforming numbers from one base to another.

1. Base b expansions of n: $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$

2. Example: 237 in decimal representation is $237 = 2 \cdot 10^2 + 3 \cdot 10^1 + 7 \cdot 10^0$ and 9 in binary is $9 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 2^3 + 2^0$

3. Binary (base 2) expansions integers are bit strings that represent the particular integers, and they are used by computers to represent and do arithmetic with integers

4. Hexadecimal expansion of also used by computer. It uses $0, 1, \ldots, 9, A, B, C, D, E, F$

5. Bytes are bit strings of length 8

6. Base conversion (expressing n base b):
   - $n = bq_0 + a_0$ $(0 \le a_0 < b)$ and a_0 is the rightmost digit of n base b
   - $q_0 = bq_1 + a_1$ $(0 \le a_1 < b)$ and a_1 is the 2nd digit from the right of n base b
   - repeat to find $a_2, a_3, \ldots$ until $q_i = 0$ for some i
7. converting from binary to hexadecimal: each hexadecimal digit corresponds to a block of 4 digits
8. binary addition: let $a = (a_{n-1}a_{n-2}\ldots a_1a_0)$ and $b = (b_{n-1}b_{n-2}\ldots b_1b_0)$. Then
   - $a + b$ is found using the usual method of adding two numbers modulo 2
   - $ab = a(\sum_{i=0}^{n-1} 2^i) = \sum_{i=0}^{n-1} a2^i$, where multiplying a by 2^i is adding i zeros at the end of a ($i.e.$ $101 \times 2^3 = 101000$) (look at the example on top left of page 225)
9. Euclidean Algorithm: gives an alternative way to find the gcd of two numbers without using the prime factorization of the two numbers.

3.7 Applications of number theory

1. writing the $\gcd(a, b) = d$ as a linear combination $d = \alpha a + \beta b$, for some $\alpha, \beta \in \mathbb{Z}$
2. if a and b are relatively prime, then $1 = \alpha a + \beta b$, for some $\alpha, \beta \in \mathbb{Z}$
3. if p is a prime such that $p|(a_1 \cdot a_2 \cdot \ldots \cdot a_n)$, then $p|a_i$ for some i $(1 \le i \le n)$
4. simplifications: if $a, b, c, m \in \mathbb{Z}$ $(m > 0)$ and $\gcd(c, m) = 1$, then
$$ac \equiv bc (\bmod m) \Rightarrow a \equiv b (\bmod m)$$
5. however, if $\gcd(c, m) \neq 1$, the above result doesn't hold (see Example 2 page 234)
6. linear congruence: $ax \equiv b (\bmod m)$ (where $a, b, m \in \mathbb{Z}$ $(m > 0)$ and x is the variable)
7. $\overline{a}$ (or a^{-1}) is the inverse of a modulo m if $\overline{a}a \equiv 1 (\bmod m)$
8. Chinese Remainder Thm (solving systems of linear congruences): for relatively prime numbers m_i, the system
$x \equiv a_1 \bmod m_1$

$x \equiv a_2 \bmod m_2$

$\vdots$

$x \equiv a_n \bmod m_n$

has unique solution modulo $m = \prod_{i=1}^{n} m_i$, namely

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n,$$

where $M_i = \frac{m}{m_i}$, and y_i is the inverse of M_i modulo m_i

9. Fermat's Little Thm: If p is a prime, and $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$ (or for any prime p, $a^p \equiv a \bmod p$).

10. the converse of Fermat's Little Thm doesn't hold since there are some composite numbers n called pseudoprimes, such that in the form $a^{n-1} \equiv 1 \bmod n$, for example $n = 341$.